

Continuation of Application for Search Warrant

I, James J. Shaw, being duly sworn, state as follows:

I. Introduction

1. I make this Continuation as part of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property – namely, a silver and green iPhone as described more fully in Attachment A (“**Subject Device 1**”) that is currently in the possession of law enforcement, and the extraction of electronically stored information from that property as described in Attachment B.

2. I am a Special Agent with the Drug Enforcement Administration, (“DEA”), a position I have held since July 2017. As part of my duties, I investigate criminal violations of the federal drug trafficking laws. I have been involved with various electronic surveillance methods, the debriefing of defendants, informants, and witnesses, as well as others who have knowledge of the distribution, transportation, storage, and importation of controlled substances. I have received training in the area of drug investigations, money laundering, financial investigations, and various methods that drug dealers use in an effort to conceal and launder the proceeds of their illicit drug trafficking enterprises. I have participated in investigations that have led to the issuance of search warrants involving violations of drug laws. These warrants involved the search of locations, including residences of targets, their associates, and relatives; storage facilities; smartphones; and computers. Evidence searched for, and recovered, in these locations has included

controlled substances, records pertaining to the expenditures and profits realized therefrom, monetary instruments, firearms, and various assets that were purchased with the proceeds of the drug trafficking. In connection with my official duties, I investigate criminal violations of Title 21, United States Code, Sections 841, 843, 846, 952 and 960, among other codified narcotics crimes, as well as violations of Title 18, United States Code, Sections 1956 and 1957, and Title 31 United States Code, Section 5332.

3. Because this Continuation is for the limited purpose of establishing probable cause to support the issuance of a search warrant for **Subject Device 1** it contains only a summary of relevant facts. I have not included each and every fact known to me or to other law enforcement officers concerning the entities, individuals, and events described in this Continuation.

4. The statements contained in this Continuation are based in part on: (a) my personal participation in this investigation; (b) information provided by other federal and state law enforcement officers, including members of the Lansing Police Department; (c) laboratory analysis reports; (d) surveillance reports; (e) criminal history records; (f) information from confidential informants; and (g) my training and experience and the training and experience of other law enforcement agents.

II. Overview of Investigation

5. This Continuation is based on the DEA investigation into the drug trafficking activities of Jason DEMYERS, a/k/a “Smooov,” and his criminal associates, including Che DEMYERS, Franchot BARNES, Jamar GOINS, Mark WILLIAMS,

Jonathan CONNER, Jomo GRADY, and Merria WALLACE, as well as other persons known and unknown. Together, these targets are part of a Drug Trafficking Organization (“DTO”) operating throughout the United States, including, but not limited to, Phoenix, Arizona; Los Angeles, California; Detroit, Michigan; and Lansing, Michigan.

6. On November 28, 2023, a grand jury sitting in the Western District of Michigan charged Jason DEMYERS, Che DEMERS, BARNES, GOINS, WILLIAMS, CONNER, GRADY and WALLACE with multiple felony counts, including Conspiracy to Distribute and Possess with Intent to Distribute Cocaine, in violation of 21 U.S.C. §§ 846 and 841(a)(1), as well as substantive drug trafficking counts, in violation of 21 U.S.C. § 841(a)(1). *See* Case No. 1:23-cr-00098-JTN. The charges arose after DEMYERS and his co-conspirators facilitated the transportation of approximately ten kilograms of methamphetamine in October 2022 and facilitated the purchase of approximately two kilograms of cocaine in June 2023.

7. On November 28, 2023, United States Magistrate Judge Ray Kent of the United States District Court for the Western District of Michigan issued arrest warrants for GRADY, WALLACE, and other co-conspirators.

8. GRADY’s criminal history includes a federal conviction for aiding and abetting possession with intent to distribute cocaine in the Northern District of Ohio (Case No. 5:15-cr-382). He was also sentenced to an additional term of imprisonment for violating the terms of his federal supervised release by, among other violations,

attempting to possess with intent to distribute methamphetamine contrary to 21 U.S.C. §§ 841(a)(1), (b)(1)(A)(viii) and 846.

III. Probable Cause

A. GRADY's Historical Use of Cell Phones to Communicate about Drug Trafficking

9. Based on my training, experience, and familiarity with the investigation, I know that drug traffickers use their cellular phones to communicate about drug trafficking. I also know that drug traffickers frequently utilize more than one cellular phone to conduct their illegal activities in an effort to thwart detection by law enforcement.

10. Specifically, I know that GRADY used cellular telephone to arrange drug deals and to communicate with fellow drug traffickers as part of the drug trafficking conspiracy with which he is currently charged. For example, GRADY was arrested during a controlled delivery of a package shipped by the DTO containing approximately ten kilograms of methamphetamine in October 2022. After receiving the package, GRADY used telephone number (269)588-9913 to communicate via Facetime with Jason DEMYERS.¹ Incident to his arrest, investigators seized multiple cell phones that were in GRADY's possession. The phones contained evidence of criminal behavior, including drug trafficking. For example, GRADY communicated

¹ Law enforcement had intercepted the package and replaced the methamphetamine inside with fake methamphetamine before executing the controlled delivery. It was this delivery that generated the supervised release violation concerning attempted possession with intent to distribute, as discussed above in the paragraph concerning GRADY's criminal history.

with his sister, with whom he was staying, about plans to deceive GRADY's probation officer about the location of GRADY's bedroom in anticipation of a home visit by GRADY's probation officer. Besides this, GRADY's devices included records of incriminating search inquiries including, "How long does FEDEX ground take Cali to Michigan;" "meth molecular structure;" and "Lansing fentanyl cocaine mixture deaths."

11. Investigators arrested GRADY after executing the controlled delivery. Following his arrest, GRADY utilized recorded jail phone systems to contact other members of the DTO (Che DEMYERS, Jason DEMYERS, and Evette WALALCE) and to coordinate the delivery of letters bound for Evette WALLACE. During review of the aforementioned calls and letter, investigators were able to confirm GRADY was accepting the methamphetamine on behalf of the DTO to transfer to a retail narcotics distributor, Evette WALLACE, for sale in furtherance of the DTO.

B. GRADY's Arrest on November 30, 2023

12. On November 30, 2023, investigators conducted surveillance of the manufacturing center located at 4971 Clay Always SW, Grand Rapids, Michigan to attempt to execute the aforementioned arrest warrant for GRADY. This is the address of GRADY's employer which was confirmed with GRADY's Federal Probation Officer. At approximately 9:20 a.m., investigators located GRADY at his place of employment sitting within a silver in color Volkswagen Passat registered in the state of Michigan to GRADY.

13. GRADY exited the parked vehicle and surrendered himself to law enforcement without incident. After which, GRADY requested investigators retrieve

his silver and green in color Samsung cellphone from within the vehicle, later identified **Subject Device 1**. GRADY provided the passcode to access the phone with the limited purpose of allowing investigators to contact Evette WALLACE to retrieve his personal belongings and take possession of the vehicle. Investigators utilized the number retrieved from GRADY's phone to arrange the transfer of GRADY's property to WALLACE on the following day.

14. On December 1, 2023, investigators met with WALLACE to release custody of GRADY's property and vehicle. During that time, WALLACE agreed to speak with investigators regards to her involvement with GRADY and the DEMYERS DTO. WALLACE advised that she had recently left a rehabilitation program and reconnected with GRADY. During that time, GRADY requested WALLACE reach out to individuals who were in debt to her from previous narcotics sales to collect currency that could be used restart retail narcotics distribution. Additionally, WALLACE advised that GRADY had utilized his cellphone to reach out to Che DEMYERS in order to reconnect to Jason DEMYERS.

15. According to U.S. Probation Officer Brett Snyder, GRADY was released from custody and began supervised release on November 9, 2023, and he was arrested on November 30, 2023. From this, I infer that this is the time period in which Evette WALLACE could have reconnected with GRADY and seen him using **Subject Device 1** as described above.

C. Probable Cause to Search the Subject Device

16. As shown above, GRADY uses cellular telephones to communicate with other members of the DEMYERS DTO and to facilitate drug trafficking activity.

17. I know from training and experience that drug traffickers frequently utilize mobile telephones to facilitate drug transactions. Drug traffickers rely upon voice phone services, SMS and MMS text messaging, social media instant messaging services, and electronic mail apps to communicate with suppliers, customers, and confederates. Mobile telephones are portable and phone providers often do not require purchasers or users of the devices to provide their true names and/or addresses, so drug traffickers often maintain multiple devices to avoid detection by law enforcement. Mobile phones often contain evidence indicative of drug trafficking, including records of incoming and outgoing calls; text messages; photographs of narcotics, coconspirators, or currency; and, in the case of “smart phones,” Global Positioning System (“GPS”) data indicating the location of the device at given points in time.

18. Based on my training and experience, I know that electronic devices such as **Subject Device 1**, can be used to store electronic information for long periods of times, including years. Even if a drug trafficker is being cautious of law enforcement detection and deleting the substance of communications, significant data may still remain on the phone, such as call logs, contact information, photographs, wireless internet connections (which can reveal location information), and other location information.

19. Further, based upon my training, experience, and participation in drug investigations and financial investigations relating to drug investigations, I am aware of the following:

- a. Drug traffickers often keep names, aliases, and/or contact information of suppliers, purchasers, and others involved in drug trafficking in their devices;
- b. Drug traffickers sometimes use electronic messaging or messaging apps, in addition to MMS, SMS text messages, and voice call, to communicate with suppliers, purchasers, and others involved in drug trafficking on their devices;
- c. Drug traffickers often take pictures or videos of their drug trafficking associates, drugs, money and/or firearms, which they store on their devices;
- d. Drug traffickers often maintain, on hand, large amounts of currency in order to maintain and finance their on-going narcotics business and often store information related to the profits of their narcotics trafficking on their devices;
- e. Global Position System (GPS) data on phones may show the location of a drug trafficker at a given time, which may provide corroborating evidence of a drug delivery or other instance of drug trafficking;
- f. User attribution data and usernames, passwords, documents, and browsing history can provide evidence that the device is being used by a drug trafficker and can provide other useful evidence to the drug investigation;
- g. Drug traffickers often use the Internet to look up various information to support their drug trafficking activities on their devices;
- h. Drug traffickers often have unexplained wealth and assets as they do not have a job, nor do they report income on their state or federal tax returns. Subjects often use cash, money orders, and cashier's checks, and prepaid debit cards as a way of purchasing items as a way to disguise where the funds are ultimately coming from. Subjects will place assets in the names of nominees, which

are often friends and family members in an attempt to hide the true ownership of the assets. It is common for drug traffickers to maintain books, records, receipts, notes, ledgers, receipts relating to the purchase of financial instruments and or the transfer of funds, and other papers relating to the transportation, ordering, sale and distribution of controlled substances. That the aforementioned books, records, receipts, notes, ledgers, etc., are maintained where the traffickers have ready access to them, including their devices;

- i. It is common for persons involved in drug trafficking to maintain evidence pertaining to their obtaining, secreting, transfer, concealment and or expenditure of drug proceeds on their devices. This evidence includes information related to currency, financial instruments, precious metals and gemstones, jewelry, books, records, invoices, receipts, records of real estate transactions, bank statements and related records, passbooks, money drafts, letters of credit, money orders, bank drafts, cashier's checks, bank checks, safe deposit box receipts or keys, records concerning storage lockers and money wrappers; and
- j. Drug traffickers frequently receive their supply of drugs through packages sent by U.S. Mail or third-party delivery service and frequently keep copies of tracking numbers, receipts and photographs of packaged narcotics on their devices.

IV. Technical Terms

20. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and

storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna

can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments, or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.
- f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

21. Based on my training and experience, I believe that **Subject Device 1** has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and/or PDA. In my training and experience,

examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

V. Electronic Storage and Forensic Analysis

22. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

23. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how **Subject Device 1** were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on **Subject Device 1** because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to

investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

24. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

25. *Manner of execution.* Because this warrant sought in this continuation seeks permission to examine a device that is currently in the possession of law enforcement, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant for search of the **Subject Device 1** at any time in the day or night.

VI. Conclusion

26. There is probable cause to believe that forensic examination of **Subject Device 1** will reveal electronic evidence of drug trafficking. The applied-for warrant would authorize the forensic examination of the **Subject Device 1**, listed in Attachment A, for the purpose of identifying electronically stored data particularly described in Attachment B.